KINETIC VERSUS CYBER ATTACKS: A LOOK AT INTERNATIONAL RESPONSE TO A NEW DOMAIN OF CONFLICT

by
Nicole Finkel

A research study submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August 2021

Abstract

This study looks at cyber attacks on the international level and how they may be unique from conventional domains of conflict, which in turn impact international response to such conflicts. Specifically, this study questions how the differences in the relationships between cyber and kinetic attacks affect international response. A qualitative social science study was conducted in order to evaluate the question posed. A comparative case study analysis was conducted using Georgia (2008) and Ukraine (2013-ongoing) as the case studies. Both of these conflicts displayed both cyber and kinetic attacks. Kinetic attacks, cyber attacks, and international response for each of the case studies was analyzed. The goal was to observe the applicability of 'armed attack' in each situation as well as the rate of the international response. Coding of critical primary sources related to the issue area were used as well. The primary sources used were four congressional testimonies on the conflicts used as the case studies. The main themes that were drawn out of this form of content analysis were conflict, assistance, and response.

The results of the data analysis revealed that there is a difference of response when it comes to kinetic versus cyber domain. With kinetic attacks, a conventional framework can commonly be applied and countries are prepared to respond in a direct manner whether that is with economic consequences, diplomatic intervention, verbal condemnation, and/or physical action. With cyber attacks, issues of attribution and lack of concrete nature of attacks can likely contribute to hesitation of nation states to respond to such action. As the case studies used illustrated, cyber attacks can contribute to kinetic attacks and cause damage on their own accord as well. This means that such attacks cannot be taken lightly, and an applicable framework needs

to be established. This study established the need for such a framework and paved the way to future research that needs to be considered.

Advisor: Professor Sarah Clark
Readers: Professor Oliver Fritz and Professor Todd Helmus

Acknowledgments

I would like to thank my family for always supporting me through all my educational endeavors and being understanding of the time I had to put into successfully completing this final project on my journey to receive a master's degree. In particular, I would like to thank my mom for always being my main editor and proofreader, always being honest with me when assessing my work, and guiding me in the right direction. I would not have been able to achieve this milestone without such a great support system.

Table of Contents

List of Tables

Introduction

Over the last few decades, the cyber domain has steadily emerged as a prominent area of aggression between nation states, private corporations, and non-state actors. It first started out as causing disruption to computer systems and causing confusion but has advanced as a method of stealing adversaries' sensitive information, disrupting critical infrastructure, and even causing physical destruction. One of the most well-known examples of such an attack is Stuxnet. Stuxnet was considered a major turning point in the cyber domain because it was used as a weapon to physically destroy a particular target, in this case being the Iranian nuclear facility at Natanz. Scholars have pondered over the idea of 'cyberwar' and Former Defense Secretary Leon Panetta, in 2012, warned of a 'cyber pearl harbor.' The cyber domain currently faces many unknowns involving its potential uses and its limitations. This poses many significant challenges. This paper will focus in on one of those specific challenges including how the international community should respond to cyber attacks.

The question that this paper attempts to answer is: how does the difference between cyber and kinetic attacks effect international response? Further, this seeks to analyze if a new framework for evaluating cyber conflict as opposed to kinetic conflict is required. With cyber coming to the forefront of conflicts between nations, it has become critical for the security of the United States and its allies to understand how to respond to cyber attacks imposed by adversaries in order to prevent further escalation of conflict, as well as potential loss of life and destruction of critical infrastructure. This idea was interestingly raised with the Estonia cyber attack in 2007 when Estonia questioned why its NATO allies did not come to its defense in the same manner they would have if it was conventional armed attack. Malicious actors had targeted websites that included Estonian government entities and media outlets. This occurred amid a conflict between

Russia and Estonia over the relocation of a Soviet-era statue in Tallin. There are distinctions between cyber and other more conventional forms of attack that make it difficult to decide if defense from other nation states was required in this type of situation. Therefore it is essential to evaluate those differences and how they impact international response. Attacks that followed the one that occurred in Estonia continued to raise this question and cause confusion from a lack of agreement from the international community on how to respond. This study will look specifically at two case studies that both involve cyber and kinetic aspects. The first case study that will be evaluated is Georgia 2008, in which malicious cyber activity turned to conventional warfare. The second case study that will be evaluated is Ukraine 2013[1] where there is a mixture of kinetic and cyber activity. Particularly, cyber activity is used to generate kinetic effects. The two events will be evaluated in a comparative case study analysis. Critical primary source documents from both events will also be coded in order to evaluate prominent themes in relation to the question presented in the research study.

Literature Review

Definitions

Common Article 2 of the 1949 Geneva Conventions sets forth that whenever two or more states resort to armed force it can be considered that international armed conflict exists.[2] But for international armed conflict to exist, the use of force must be conducted by the state and not by private individuals even if they are acting on behalf of the state. An armed conflict must consist of an international component and an armed component.[3] Article 49(1) found in the 1977

[1] This case study begins in 2013, but the conflict continues into present day. To maintain specificity for the purpose of this particular study, only the initial conflict (kinetic and cyber) will be evaluated. This will encompass 2013-2017.
[2] International Committee of the Red Cross, "Geneva Convention Relative to the Protection of Civilian Persons in Time of War"
[3] Ibid.

Additional Protocol I to the 1949 Geneva Conventions defines 'attacks' as "acts of violence against the adversary, whether in offence or in defense."[4] Article 2(4) of the UN Charter states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state…" It also touches on the fact that action cannot be taken in manner that is not in accordance with the goals set forth by the UN.[5] Article 51 of the UN Charter puts forth that states have a right to collective self-defense if an armed attack occurs against a member of the United Nations.[6] One of the current issues when it comes to the cyber domain is lack of clarity of terminology and key terms. In order to have a clear understanding of what is being discussed further in this research project, specific definitions will be put forth in accordance with the National Initiative for Cybersecurity Careers and Studies, an initiative of the Cybersecurity and Infrastructure Security Agency. Critical infrastructure is "the systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters."[7] Cyberspace is "the interdependent network of information technology infrastructures that includes the internet, telecommunication networks, computer systems, and embedded processors and controllers" (cyberspace and cyber domain may be used interchangeable in this paper).[8] According to the National Research Council, there are a variety of definitions for cyberattack, but the one that will be used is "a hostile or unfriendly action taken against a computer system or network regardless

[4] International Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts"
[5] United Nations, "Charter of the United Nations," Article 2.
[6] United Nations, "Charter of the United Nations," Article 51.
[7] National Initiative for Cybersecurity Careers and Studies, "Cybersecurity Glossary"
[8] National Initiative for Cybersecurity Careers and Studies, "Cybersecurity Glossary"

of purpose or outcome.[9] But also, it is important to note that a hostile cyber operation can be an exploitation or an attack. A cyber exploitation is "an action intended to exfiltrate digitally stored information that should be kept away from unauthorized parties that should not have access to it."[10]

International Legal Understanding of Cyber Attacks

In the modern setting, legal scholars have evaluated the applicability of certain doctrines to cyberspace. For some time, the main view of nation states which are members of the United Nations has been that force and armed conflict (as put forth in the UN charter) applies to military attacks or violence. Alternatively, Article 2(4) can be looked at from the perspective of what instruments are used or the rights of individuals that are at stake. [11] Under Article 51, if a cyber attack is classified as an 'armed attack' it can be deemed legal to use force to retaliate in self-defense, or in defense of UN allies. One of the key factors involved in Article 51 and a deciding factor in whether self-defense is applicable is the characteristic of imminence.[12] Under the Obama Administration, in a legal review, it was put forth that the United States has the power to conduct strikes when an armed attack is imminent specifically in the cyber context. It has been made clear, via the broad agreement by scholars, that cyber attacks that result in death or physical destruction of critical infrastructure fall under the Article 51 definition of and armed attack.

The Tallinn Manual, originally published in 2013, served to address cyber operations and how the rules of international law can govern such incidents. The experts that put together the

[9] National Research Council, "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," 29-52.
[10] Ibid.
[11] Matthew C. Waxman, "Cyber Attacks as 'Force' Under UN Charter Article 2(4)," 43-54.
[12] Ryan J. Hayward, "Evaluating The 'Imminence' Of A Cyber Attack For Purposes Of Anticipatory Self-Defense."

Tallinn Manual had two perspectives on how a cyber attack may fall under the category of an 'armed attack.' First, the Tallinn Manual puts forth that "any use of force that injures or kills persons or damages or destroys property" would qualify.[13] This point had unanimous agreement from the experts that put together the Tallinn Manual. The second point, which also holds significant weight to it but did not have unanimous support, was that its applicability to an 'armed attack' could be determined by its scaled of negative consequences imposed, even if death or direct destruction is not involved.[14] Some scholars argued that this opened the door to less clarity and more confusion on what would be applicable as an 'armed attack' within the cyber domain.

Some scholars argue that cyberwar is a misleading term as mixing cyberattacks with the concept of war is inaccurate.[15] On the other hand, scholars such as Michael Schmitt, one of the experts behind the *Tallinn Manual on the International Law Applicable to Cyberwarfare*, push back on that idea.[16] They see that both jus ad bellum and jus in bello can apply to cyber operations.[17] The manual emphasizes cyber operations as a new form of weapon allowing for law to be applicable to the concept. But even scholars who agree with the concept put forth by the manual argues that it is not simple to place cyber actions on a framework that easily applies to kinetic conventional attacks considering factors such as violence, physical destruction, and motive.[18] These aspects are not as easily measured when it comes to observing cyberattacks on their own, especially when the aggression involves a combination of cyber and kinetic actions.[19]

Cyberwar: Strategic Thought

[13] Michael N. Schmitt, "Tallin Manual on the International Law Applicable to Cyber Warfare."
[14] Ibid.
[15] Christopher Finlay, "Just War, Cyber War, and the Concept of Violence," 357-376.
[16] Michael Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," 283- 293.
[17] Ibid.
[18] Christopher Finlay, "Just War, Cyber War, and the Concept of Violence," 357-376.
[19] Ibid.

Most, if not all, scholars recognize that one of the key differences between the cyber domain and conventional domains of warfare (sea, land, air, and space) is that there is no concrete space in which it takes form. Cyberspace is a replicable construct which means it can take many shapes in a variety of unique locations. Some scholars have chosen to compare the unique nature of cyberwar to nuclear war with dramatic long-term effects, but scholars such as Libicki have pushed back on that claim viewing cyberwar as temporary and rapidly over.[20] Bayles saw similarity between chemical and biological weapons and cyber weapons because of the large number of people they could target at the same time, but saw the key difference being that cyber weapons affect individuals indirectly rather than directly.[21] The differences between the cyber domain and conventional domains of warfare also highlight the parallel between the cyber domain and other forms of asymmetric domains of conflict. Looking at non-conventional forms of attack such as disinformation campaigns, use of biological or chemical weapons, or targeted killings, a lack of concrete nature and the unique nature of direct and indirect effects can also be noted.

Rid, when assessing the concept of cyberwar, brings in the fundamental concept of war put forth by Clausewitz. Clausewitz categorizes war by its violent nature, instrumental character, and political nature.[22] Rid agrees with this categorization and sees an act of force as straightforward in nature. He gives examples of F-16 striking targets or improvised explosive devices playing to the same end goal.[23] The end goal, in Clausewitz view, is when the enemy is forced to accept their lose and whatever consequences that may entail. Rid argues that cyberwar falls into a completely different category, opposed to conventional forms of war, as the act of

[20] Elinor C. Sloan, "Modern Military Strategy: Cyberwar," 142-159.
[21] Ibid.
[22] Thomas Rid, "Cyber war will not take place: what is cyber war," 2013.
[23] Ibid.

force when it comes to cyber is not as clear and direct.[24] A cyber attack involves a complex chain of events, causes, and consequences (direct and indirect). Rid takes Clausewitz criteria for use of force of war and deems that cyber cannot meet all the criteria[25], and therefore cyberwar is unlikely to become a reality.[26] In essence, malicious cyber activity will occur, but categorizing it as cyberwar will prove to be nearly impossible under the given criteria. On the other hand, scholars such as Junio and Liff argue that there is a possible criteria under which cyberwar can, and likely will, occur. Liff sees the possibility of cyberwar capabilities potentially increasing the frequency of war and conflict on the international stage.[27] But Liff does not see such capabilities encouraging kinetic warfare under most circumstances. In other words, he sees acts of cyberwarfare occurring between actors in the context of larger political conflict, which makes the role of cyber actions less significant to the overall conflict.[28] Junio sees cyberwar as a highly costly and probable event; within this definition cyberwar is something that can involve a variety of consequences ranging from destruction of military capabilities to destruction of critical infrastructure.[29]

The US Cyber Command sees the principal effect of cyber warfare as denying the enemy freedom of action in the cyber domain.[30] The strategic goal of offensive cyberwar can include coercion, assertion of status, or disabling capabilities of an enemy. Various scholars have pointed to the fact that cyberwar is a supporting form of warfare, and the US Cyber Command seems to

[24] Ibid.
[25] The criteria are the 3 elements of war discussed earlier: violent, instrumental, and political. Rid argues that there are little examples of cyber attacks that meet one of the elements and no examples of cyber attacks that meet all of the elements.
[26] Thomas Rid, "Cyber war will not take place: what is cyber war," 2013.
[27] Adam P. Liff, "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio," 134-138.
[28] Ibid.
[29] Timothy J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," 1-8.
[30] Elinor C. Sloan, "Modern Military Strategy: Cyberwar," 142-159.

back up this assertion by putting forth that cyber weapons can mainly be used in combination with conventional military operations.[31]

Relationship Between Cyber Attacks and Kinetic Attacks

There are several key differences between cyberspace and kinetic attacks, or further between cyberwarfare and conventional warfare. As mentioned previously, one key difference is the lack of concrete space in which cyberspace falls into. Another difference is that a cyberattack has the potential to cause widespread damage in a very short period of time that can affect the functioning of society and lead to indirect casualties. The rapid nature and the ability to attack anywhere at any time increases the risk involved in cyberspace.[32] The cyber battlefield is also seen as unique because it does not necessarily require the same level of training and education as forms of conventional warfare require. Phillips highlights that this is why many non-state actors engage in cyber warfare. [33]Cyber attacks occur quickly and with little to no warning. But, they also come to an end quickly as soon as the vulnerability is corrected. Meanwhile, kinetic weapons are durable and can remain effective for a long period of time. For such reasons, Phillips view cyberwarfare as asymmetric in comparison to the conventional domains of war.[34]

Libicki argues that incidents of cyberattacks transitioning to kinetic attacks have so far been proven quite unlikely by lack of evidence of such.[35] He sees it as something that may occur, but with low probability. He also argues that cyberattacks would be less likely to cause a kinetic response because of their generally non-lethal nature and recovery rate.[36] Other scholars argue that the concept of 'kinetic cyber attacks' have been around for about a decade and that such

[31] Elinor C. Sloan, "Modern Military Strategy: Cyberwar," 142-159.
[32] Ibid.
[33] Andrew Phillips, "The Asymmetric Nature of Cyber Warfare," 10-11.
[34] Ibid.
[35] Martin Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks," 199-211.
[36] Ibid.

attacks have been validated via the laboratory and in the operational environment. An example that is used is Stuxnet which was targeted malware used to destroy physical devices.[37]

Another contrast, that scholars highlight, between the cyber domain and the conventional domains of warfare is that cyberspace is 'man-made.' It can evolve very quickly under the discretion of various actors. The cyber domain is filled with a variety of actors from both the public and private domain and tracing the activity of such actors is not easy give the lack of structure. Scholars, such as Handler and Patterson, highlight that attribution is a key issue when it comes to differentiating between cyber and kinetic attacks. Patterson raises two challenges that attribution creates in the cyber domain.[38] First, determining the identity of the actor behind the attack is challenging and often time consuming. Second, identifying whether the actor behind the attack is working in coordination with a nation state or is with a criminal non state entity group. The response for each type of attack would likely differ. Handler sees cyberspace as an active battleground for individuals, crime organizations, nation states, and other non-state actors (such as terrorist organizations. In addition to the identification problem that Patterson emphasizes, Handler also sees the attribution problem involving difficulty to determine intent and at what point do states get held responsible for malicious cyber activity that occurs within their borders.[39]

Cyber Domain: A New Framework?

One the biggest debates among scholars surrounding the cyber domain is how applicable the existing framework of conventional war domains is to the cyber realm. There are multiple layers to this debate[40] with some scholars arguing that cyberwar will never happen. But it is clear

[37] Scott Applegate, "The Dawn of Kinetic Cyber"
[38] Ryan Patterson, "Silencing The Call To Arms: A Shift Away From Cyber Attacks As Warfare," 969-983.
[39] Stephenie G. Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends In Warfare," 209- 237.
[40] As discussed in the literature review subsection entitled "Cyberwar: Strategic Thought"

that the cyber domain is a space of conflict whether or not one can see that progressing to full out war.

Some scholars consider cyberspace a fifth operational domain. Welch argues that the cyber domain needs to be treated like a place, just like other domains of war, in which military actions create some form of intended results.[41] A nation state needs to be prepared to defend itself and conduct offensive mission in cyberspace, just like they may do on land, air, or sea. Considering cyberspace as another operational domain, some scholars argue that it will add new rules to the battlefield just like technological advancements have done in the past.[42] For example, the time period between World War I and World War II brought long-range aircraft and radio coordinated ground-to-air attack methods. Hughes argues that such changes do not just bring an adjustment to an already existing framework of war but call for a completely new legal framework.[43] He goes even beyond that to argue that a concrete framework may be difficult to develop in cyberspace due to the fluid nature of technology. He uses the lack of application of the international humanitarian law (IHL) to cyber as an example.[44] Schmitt, one of the authors behind the Tallin Manuel, sees existing legal framework applying to the cyber domain with some adjustments.[45] Others, like Dipert, argue that legal frameworks are often problematic and not as applicable as should be to specific situations.[46]

Looking Forward

There are a few common themes that can be drawn away from existing scholarship in this area of study. First, it is clear that a major issue in the cyber domain is lack of concrete

[41] Gen. Larry D. Welch, "Cyberspace: The Fifth Operational Domain," 2-7.
[42] Rex Hughes, "Towards a Global Regime for Cyber Warfare," 106- 116.
[43] Rex Hughes, "Towards a Global Regime for Cyber Warfare," 106- 116.
[44] Ibid.
[45] Michael N. Schmitt, "Tallin Manual on the International Law Applicable to Cyber Warfare."
[46] Randall R. Dipert, "The Ethics of Cyberwarfare," 284-410.

definitions and lack of applicability to existing framework like the definitions that are put forth by the UN Charter. Second, there are several key differences between cyber and kinetic attacks. Most center around the factor that the cyber domain is less concrete and allows more flexibility and less predictability for a variety of actors. This lack of concrete domain gives way to the difficulty of attribution which may play a key role in response by other nations or organizations. Finally, most scholars agree that the cyber domain has a role in warfare. The disagreement comes in on how large of an impact that role has and whether it has a direct impact on kinetic warfare. After reviewing the existing literature surrounding the question of the differences between kinetic and cyber attacks and how that impacts response, it is possible to predict that this study will show a lack of a concrete framework specific to cyber attacks playing an impact on lack of response by the international community.

Methodology and Hypothesis

To reiterate, the question that this study seeks to evaluate is how does the difference between cyber and kinetic attacks effect international response. The key idea behind this question is to understand the reason why response rate might be different and how that further impacts what occurs after a cyber attack. Based on existing literature and debate in the field, it is possible to hypothesize that due to the lack of concrete nature to the cyber domain and lack of applicability of the current conventional warfare framework, the response to cyber attacks is not as direct and persistent as with conventional attacks.

A qualitative social science method of research will be used to evaluate the question and test the above hypothesis. A comparative case study approach paired with coding evaluation of key primary sources in the field has been chosen as the most effective method of testing for this research. This will allow for the proper evaluation of the relationship and comparison of kinetic

and cyber attacks. The cyber domain is a rapidly evolving field with many actors involved with various intentions. Due to the lack of concrete framework in the field, it is best to look at recent, real incidents that occurred on the international platform. Two case studies involving Russia were chosen for the purpose of minimizing the variables involved. The first case study focuses on the Russo-Georgian War in 2008 where malicious cyber action transitioned to kinetic warfare. The second case study focuses on the conflict between Russia and Ukraine that began in 2013 and continues to this day. This conflict involves both cyber and kinetic activities. These case studies were chosen because they involve both cyber and kinetic action which allows for evaluation of how they may impact each other, and when response from the international community is most pronounced. For the comparative case study component, information will be gathered from news articles and primary sources such as press releases. The subsections for each case study will be broken up into background/kinetic attacks, cyber attacks, and international response. This will allow for comparison of each key issue area for the case study analysis. The variables that will be considered when evaluating both case studies are whether the attack falls into the legal framework for 'armed attack' and the level of response from the international community. For an 'armed attack' to exist[47] there needs to be an international component to the conflict and there needs to be an armed use of force component to the conflict. The discussion of data will aim to analyze whether or not the attack had an international component and if there was use of armed forced based on the background provided in the case study. The level of response will be ranked with the options being *none*, *verbal condemnation*, *physical intervention*. The ranking will be drawn from the *international response* section of the case study.

[47] Refer to "Literature Review: Definitions" section for further guidance.

For the coding component of the data analysis, four congressional hearings will be used. Congressional hearings were chosen as the primary source type for content analysis because it would allow for a better understanding of how the United States envisions response to such conflict issues. In addition, it would likely highlight what the United States sees as the role of the international community in responding to conflict. Understanding both kinetic and cyber conflicts and the necessary response for both is crucial for the security of the United States, so it provides insight for the purpose of this research project to understand their perspective on the conflict and response. Two of the congressional hearings focus on Georgia.[48] The other two hearings take a look at the situation in Ukraine.[49] The coding will draw on key themes that are seen in all four of the documents in an effort to see what discussion topics were prioritized during the congressional hearings and how that may impact the response to the case studies evaluated in this research.

There will be several key factors to consider in order to evaluate if the hypothesis that has been put forth is correct. First, the circumstances of the case study must meet the definition of an 'armed attack' at some point in time. If there is an international component and use of force or violence component, then the circumstances can be considered an 'armed attack' for purposes of this research. Both kinetic and cyber attacks should ideally fall under this categorization, but due to the lack of concrete barriers in the cyber domain data analysis will show that cyber attacks are not categorized under the current framework of an 'armed attack.' Second, if the hypothesis follows correctly, the international response should rank higher for kinetic attacks than for cyber

[48] The first hearing before the Committee on Foreign Relations United States Senate is entitled "Russia's Aggression Against Georgia: Consequences and Response" The second hearing before the Committee on Armed Services United States Senate is entitled "The Current Situation in Georgia and Implications For U.S. Policy"
[49] The first hearing before the Committee on Foreign Relations United States Senate entitled "Developments in Ukraine" The second hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services United States Senate entitled "Russian Influence and Unconventional Warfare Operations In The 'Gray Zone': Lessons From Ukraine"

attacks. Finally, the coding will have to show an increased focus on kinetic attacks and response than focus on the cyber domain. Overall, in order to view the hypothesis, put forth, as accurate there will need to be a clear focus on the kinetic as opposed to the cyber and this will be seen as directly impacting the response.

Data

Case Study 1: Georgia (2008)

Background and Kinetic Attacks

The war between Georgia and Russia in 2008 lasted for about a week, but the rising tensions stemed from years before. In 1990, South Ossetia declared its independence from Georgia.[50] Just a year later, Georgia declared independence from the Soviet Union and shortly after civil war broke out in the newly independent country. Abkhazia declared its independence from Georgia in 1992.[51] After conflict between Abkhasian separatist and Georgian military a ceasefire was agreed upon in 1994 and peace was maintained until 2001.[52] In September of 2002, Putin demanded that Georgia respond to accusations that they were harboring Chechen militants.[53] In 2006, South Ossetians demanded independence. In 2007, Russia withdrew troops from Georgia. Their presence remained for peacekeeping purposes in Abkhazia and South Ossetia.[54] Geographically, South Ossetia borders with Russia and residents are primarily Russian speaking. In August 2008, tensions between the two countries intensified over the South Ossetia region amongst talks of Georgia and Ukraine joining NATO.[55] At the end of May, Russia sent hundreds of unarmed troops to Abkhazia which Georgia interpreted as a setup for military

[50] CNN Editorial Research, "2008 Georgia Russia Conflict Fast Facts," *CNN World.* https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] CBS, "Russia Bombs Georgian Targets," *CBS.*

intervention.[56] On August 7th, Georgia sent troops to South Ossetia and Russia moved troops to the border and began air strikes in South Ossetia.[57] By August 10th, Russian troops proceeded to move further into Georgia. The military action, which included intense bombing, came to an end on August 12th in what looked like a clear Russian victory.[58] Both sides experienced many casualties, including civilian causalities.[59] A ceasefire was negotiated in which President Medvedev of Russia promised recognition of independent Abkhazia and South Ossetia.[60] The EU conducted an independent international fact-finding mission on the conflict in which it was concluded that both sides contributed to the conflict.[61] Georgia initiated the first military action on the capital of South Ossetia on August 7th, but the blame could not be laid solely on them as the action was taken because of years of rising tensions and provoking incidents.[62]

Cyber Attacks

Weeks before war broke out between Georgia and Russia in August 2008, various cyber organizations based in the United States noticed malicious cyber activity targeting Georgian government websites.[63] Attacks against Georgia's cyber domain began around July 20th with distributed denial of service (DDOS) attacks, as well as infiltration of government networks with the goal of stealing sensitive information and defacement of websites with propaganda.[64] The main target of the attacks was the government, but media, communications, and transportation

[56] Ibid.
[57] CNN Editorial Research, "2008 Georgia Russia Conflict Fast Facts," *CNN World.*
[58] Ibid.
[59] Reuters Staff, "Factbox: Facts about the 2008 War in Georgia," *Reuters*, https://www.reuters.com/article/us-georgia-war-conflict-sb/factbox-facts-about-the-2008-war-in-georgia-idUSTRE5732TH20090804.
[60] Ibid.
[61] European Union Council, "Independent International Fact- Finding Mission on the Conflict in Georgia," EU.
[62] Ibid.
[63] Joseph Nye, "Only a credible threat of response can deter cyber."
[64] John Markoff, "Before the Gunfire, Cyberattacks," https://www.nytimes.com/2008/08/13/technology/13cyber.html.

companies were also targeted.[65] Georgia placed blame on Russia for the attacks, although Russia denied government involvement.[66] According to cyber researchers, there seemed to be evidence connecting the malicious actions in the cyber domain to a Russian criminal gang known as the Russian Business Network (RBN).[67] Computer security experts witnessed how the actors behind the malicious cyber operations staged botnets, malicious computer programs, in the lead up to the kinetic attacks. They were activated shortly before air strikes began on August 7th.[68]

International Response

The EU coordinated a ceasefire between the two fighting forces on August 12th.[69] Russia recognized the regions of Abkhazia and South Ossetia as independent and both countries agreed to withdraw forces to their pre-war positions. But Russian troops remained in the area, and took control of the established borders at the time.[70]

International intervention into the conflict began on August 8th when the United States, United Kingdom, and NATO called for a cease fire of military hostilities by both countries.[71] Just a day later, a delegation of diplomats from EU and the US went to Georgia in an effort to mitigate rising military tensions.[72] There was international consensus from the West that Russia's response was inappropriate. As a result, NATO and the EU disconnected with Russia, a

[65] Ibid.
[66] Ibid.
[67] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government," https://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.
[68] John Markoff, "Before the Gunfire, Cyberattacks."
[69] Reuters, "Factbox: Facts about the 2008 war in Georgia," https://www.reuters.com/article/us-georgia-war-conflict-sb/factbox-facts-about-the-2008-war-in-georgia-idUSTRE5732TH20090804.
[70] Ibid.
[71] CNN Editorial Research, "2008 Georgia Russia Conflict Fast Facts," https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html.
[72] Ibid.

silence that lasted for about a year. The United States also sent ships to deliver aid to Georgia, in addition to the $4.5 billion that was offered in aid.[73]

Ukraine (2013- Ongoing)[74]

Background and Kinetic Attacks

Unrest at the end of 2013 with protests against President Viktor Yanukovych led into violence and chaos in 2014.[75] One of the most critical tensions points between Russia and Ukraine at the time was Ukraine's growing relationship with the European Union (EU). With increasing unrest and pressure, Yanukovych discarded the idea of formalizing a tighter economic relationship with the EU.[76] At the same point, Russia was putting pressure on Ukraine to join the Eurasian Economic Union, which was just a concept at the time.[77] With the ousting of Yanukovych from power, Russia saw an opportunity to reestablish its influence over Ukraine. Russian forces invaded Crimea on February 27th and increased their presence over bases in the region. Amid an unstable interim government in Ukraine, protests erupted in Crimea in March 2014.[78] Putin used force to protect Russian interests in the region. At that point, the Ukraine government deemed that Russia had launched a war against it. On March 25th, interim Ukrainian president Turchynov ordered the withdrawal of military forces from Crimea after Russian troops had taken over all the military bases.[79]

In the eastern cities of Donetsk, Luhansk, and Kharkiv, protests erupted in coordination with occupation of buildings. The government struggled to tame the protestors and the Russian

[73] Reuters, "Factbox: Facts about the 2008 war in Georgia," https://www.reuters.com/article/us-georgia-war-conflict-sb/factbox-facts-about-the-2008-war-in-georgia-idUSTRE5732TH20090804.
[74] The conflict in Ukraine is still ongoing and it is noted so in the subheading but the focus of case study and analysis to follow will look at the kinetic and cyber aggression in the time range of 2014-2017.
[75] BBC, "Ukrainian Crisis Timeline," https://www.bbc.com/news/world-middle-east-26248275.
[76] Jonathan Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia."
[77] Ibid.
[78] BBC, "Ukrainian Crisis Timeline," https://www.bbc.com/news/world-middle-east-26248275.
[79] Ibid.

government used this to their advantage in calling out the Ukraine government in their inability to properly govern.[80] Russian strategy differed in these eastern regions from its more militarily forceful approach in the annexation of Crimea. In Eastern Ukraine, Russia used a political-warfare approach to undermine the influence of the Ukrainian government. As support for protest increased, Russia turned its focus to more conventional uses of force in Eastern Ukraine as well.[81] At that point in time, Russia did not meet its goals in influencing the Ukrainian government to certain concessions. Tensions did not subside between the two countries. Ukrainian elections on May 25th, 2014 brought Petro Proshenko into power.[82] It also brought him into a disorderly situation. Fighting among pro-Russian separatists and government forces intensified in April. Separatists established self-declared republics in the Luhansk and Donetsk regions.[83] Even under new leadership, by August, thousands had been killed and thousands more left their homes.[84]

Cyber Attacks

In May 2014, as physical conflict escalated between Ukraine and Russia, Ukraine's presidential election was targeted by hackers when they broke into the Central Election Commission.[85] Later in the year, hackers targeted the same entity during a parliamentary vote in October.[86] In December 2015, with the malicious cyber activity persisting, the control centers of three electricity distribution companies were hacked.[87] The hackers opened breakers at dozens of

[80] Ibid.
[81] Ibid.
[82] Council on Foreign Relations, "Ukraine in Crisis," https://www.cfr.org/backgrounder/ukraine-crisis.
[83] Ibid.
[84] Ibid.
[85] Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
[86] Ibid.
[87] Donghui Park & Michale Walstrom, "Cyberattack on Critical infrastructure: Russia and the Ukranian Power Grid Attacks," https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks.

distribution substations in the Ivano-Frankvisk region which led to over 200,000 consumers losing power.[88] The malicious actors had used a malware known as BlackEnergy to target companies with spear phishing emails that tricked employees into downloading corrupt files that led to the destruction of portions of the grid.[89] The hacking intensified in 2016. In the months of November and December alone, Ukrainian state institutions were targeted by hackers about 6,500 times.[90] On December 17, 2016, a single transmission substation in northern Kiev lost power. The power cut resulted in a loss of about one-fifth of Kiev's power consumption at that time.[91] One of the world's most financially damaging cyber attacks took place in 2017 in Ukraine. The malware, NotPetya, was used to compromise software that granted the hackers access to computer systems of utility companies, banks, airports, and government agencies. It went further to effect large corporations such as FedEx.[92] The estimated damages and recovery cost was about $10 billion dollars on an international scale.[93]

International Response

After Russia invaded Crimea in early 2014, the White House issued a warning to Russia in regard to the risk it was running of violating Ukraine's sovereignty.[94] NATO also ordered Russia to withdraw its forces from Ukraine.[95] Shortly after, the United States offered financial support to Ukraine in the form of one billion dollars in loan.[96] On March 6, 2015, President

---

[88] Ibid.
[89] Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
[90] Natalia Zinets, "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'", https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC.
[91] BBC, "Ukraine power cut 'was cyber-attack'," https://www.bbc.com/news/technology-38573074.
[92] Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
[93] Ibid.
[94] Jaewon Kang, "Here's what you need to know about Ukraine crisis," https://www.nbcnews.com/storyline/ukraine-crisis/ukraine-crisis-what-you-need-know-now-n44551.
[95] Ibid.
[96] Ibid.

Obama issued an executive order declaring a national emergency in regard to the situation in Ukraine.[97] In August, with the Ukrainian crisis nearing no conclusion, the UN security council met in an emergency session and the US national security council met at the White House.[98] The United States moved forward with more economic sanctions, but stayed away from military intervention as to not increase conflict in an already burdened military zone.[99]

Ukrainian investigators worked relatively quickly to find the perpetrators of the cyber attacks that were growing in intensity. They discovered that the hackers were Russian speaking. The grid attacks were predicted to be connected to a group called Advanced Persistent Threat 28 (APT28).[100] The group is known to have ties to the Russian government. Its record of attacks includes the Ukrainian Election Commission[101] and the U.S. Democratic National Committee. In February 2016, U.S. deputy Energy Secretary Elizabeth Sherwood- Randall attributed the 2015 attack to Russia.[102] But most U.S. officials were hesitant to do so as they felt that there was not enough evidence to come to a conclusive claim. In the aftermath, investigators discovered that APT28 may in fact not be the ones behind the 2015 attack, instead suspecting the Sandworm Team.[103] The Sandworm Team is another Russian-hacking group which has a reputation of targeting foreign government organizations.

International response intensified with the NotPetya ransomware attack that cost the world billions of dollars in damage. Although Russia denied its involvement in the attack, the

---

[97] Barack Obama, "Executive Order Declaring a National Emergency With Respect To The Situation In Ukraine."
[98] Shaun Walker, "Ukraine crisis: emergency NATO, UN, and EU meetings after Russian invasion claim," https://www.theguardian.com/world/2014/aug/28/ukraine-russia-emergency-un-nato-eu-meetings-invasion-claim.
[99] Ibid.
[100] Donghui Park & Michael Walstrom, "Cyberattack on Critical Infrastructure: Russian and the Ukrainina Power Grid Attacks."
[101] The attacks on the Ukrainian Election Commission took place in May and October 2014.
[102] Donghui Park & Michael Walstrom, "Cyberattack on Critical Infrastructure: Russian and the Ukrainina Power Grid Attacks."
[103] Ibid.

international community did not hold back in attributing the attack to them. The UK Defense Secretary at the time, Gavin Williamson, argued that Russia was breaking the rules of the international community and that the UK will not hold back in responding to such violations.[104] The United States also did not hold back on blaming the attack on Russia. The former White House Press Secretary, Sarah Sanders, represented the administration in expressing that the cyber attack was reckless and that the attackers would face international consequences.[105] A researcher at the NATO Cooperative Cyber Defence Centre of Excellence made statements on the legal issues that the perpetrators of the attack could face including a possible violation of sovereignty. The official elaborated that countermeasures taken by the international community may be justified if the attack is attributed to the state.[106]

Coding of Congressional Hearings

Close analysis and coding of the congressional testimony for both Georgia[107] and Ukraine[108] revealed key themes that emphasized trends that benefited the analysis of the issue at

[104] BBC, "UK and US blame Russia for 'malicious' NotPetya cyber-attack," https://www.bbc.com/news/uk-politics-43062113.
[105] Dustin Volz & Sarah Young, "White House blames Russia for 'reckless' NotPetya cyber attack," https://www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.
[106] The NATO Cooperative Cyber Defence Centre of Excellence, "NotPetya and WannaCry Call for a Joint Response from International Community," https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/.
[107] U.S. Congress. Senate. Committee On Foreign Relations. *Russia's Aggression Against Georgia: Consequences And Responses*. 110th Cong., 2nd sess., 2008. & U.S. Congress. Senate. Committee On Armed Services. *The Current Situation in Georgia and Implications for U.S. Policy*. 110th Cong., 2nd sess., 2008.

[108] U.S. Congress. Senate. Committee On Foreign Relations. *Developments In Ukraine*. 113th Cong., 2nd sess., 2014. & U.S. Congress. Senate. Committee On Armed Service: Subcommittee on Emerging Threats and Capabilities. *Russian Influence and Unconventional Warfare Operations in The 'Gray Zone': Lessons From Ukraine*. 115th Cong., 1st sess., 2017.

hand. The major themes observed are conflict, military[109], political[110], cyber[111], assistance, and response[112]. In order to provide a balanced analysis for all four congressional testimonies, the same common themes were applied to both the Ukraine and Georgia hearings. The documents ranged from 54-63 pages. Table 1 below is the code chart for Georgia using two congressional hearings that both took place in 2008 around the time of the conflict. Table 2 below is the code chart for Ukraine using two congressional hearings. One of the hearings took place at the beginning of the conflict in 2014 and the other hearing took place in 2017, close to the end of the conflict period that was used for the case study analysis above. The code count notes the number of times each theme is mentioned within the individual hearings (the order of which is noted in the footnote numbered next to the Table title). The bolded number in the code count is the total times the mentioned theme arises in the hearings.[113]

Table 1: Georgia Case Study Congressional Hearings Coding Table[114]

CODE NAME	Congressional Hearing 1	Congressional Hearing 2	Total
Conflict	73	42	**115**
Military	64	32	**96**
Political	8	10	**18**
Cyber	16	1	**17**
Assistance	37	38	**75**
Economical	13	17	**30**
Response	92	66	**158**

[109] For both coding tables, this category accounts for military conflict, aggression, and action related specifically to the Georgia conflict (2008) and the Ukraine conflict (2013-Ongoing).
[110] For both coding tables, this category accounts for political conflict and action related specifically to the Georgia conflict (2008) and the Ukraine conflict (2013-Ongoing).
[111] For both coding tables, this category accounts for cyber conflict, malicious activity, and aggression related specifically to the Georgia conflict (2008) and the Ukraine conflict (2013-Ongoing).
[112] This accounts for both international response and United States response.
[113] For consistency, the code count includes both verbal and written testimony presented in the hearing document. Some overlap is present.
[114] The first hearing before the Committee on Armed Services United States Senate is entitled "The Current Situation in Georgia and Implications For U.S. Policy." (Code Count 1 in Table 1) The second hearing before the Committee on Foreign Relations United States Senate is entitled "Russia's Aggression Against Georgia: Consequences and Response" (Code Count 2 in Table 1)

Table 2: Ukraine Case Study Congressional Hearings Coding Table[115]

CODE NAME	Congressional Hearing 1	Congressional Hearing 2	Total
Conflict	2	26	**28**
Military	25	41	**66**
Political	12	23	**35**
Cyber	3	33	**36**
Assistance	30	5	**35**
Economical	7	3	**10**
Response	50	38	**88**

Discussion

To reiterate the hypothesis put forth was that due to the lack of concrete nature to the cyber domain and lack of applicability of the current conventional warfare framework, the response to cyber attacks is not as direct and persistent as with conventional attacks. To evaluate this hypothesis, two case studies and content analysis via coding of primary sources were used as data. What follows is a discussion on how the data matched the criteria that was established in the methodology section above.

Is this an Armed Attack?

In the case studies, the *background/kinetic attack* and *cyber attacks* subsections provided an understanding of how adequately each scenario fits under the definition of 'armed attack' as the framework currently has it established. Two factors need to be considered: international component and whether use of force was involved. For the Georgia case study kinetic attack, it is clear that the attack had both an international component and that use of force was involved. Military forces were used by both Georgia and Russia. Military action included intense bombing

[115] The first hearing before the Committee on Foreign Relations United States Senate entitled "Developments in Ukraine." (Code Count 1 in Table 2) The second hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services United States Senate entitled "Russian Influence and Unconventional Warfare Operations In The 'Gray Zone': Lessons From Ukraine" (Code Count 2 in Table 2)

and casualties included civilian causalities. In regard to the cyber attack component of the conflict, there was an international component as it played a role beyond the borders of just one country, but it was not clear right away who was behind the attack. Georgia blamed Russia although Russia denied responsibility. It is important to recall that in order for a conflict to qualify as international armed conflict, the use of force needs to be conducted by the state.[116] This is an issue area that arises when dealing with cyber attacks where responsibility for an attack is denied by the state. The cyber attack also did not qualify as direct use of force. Instead, there was infiltration of government networks. This led to acquisition of confidential information and a stream of propaganda across several critical industries. The cyber attack, on its own, does not meet the criteria of an 'armed attack.'

For the Ukraine case study there is a similar trend. With the kinetic attacks, it is clear that there is both an international component and that use of force is involved to achieve a certain goal. Russian forces invaded Crimea at a time where the Ukraine government was vulnerable and in transition. Russia also turned to conventional use of force in Eastern Ukraine where fighting among pro-Russian separatists and government forces led to thousands of deaths. The cyber attacks, occurring on several occasions from 2014-2017, had international implications. The attackers targeted critical infrastructure within Ukraine leaving thousands without power. Again, it was not clear who the perpetrator of the attacks was. For example, Ukraine investigators first attributed the 2015 power grid hack to APT28, but later turned to The Sandworm Team as the ones behind that attack. Both groups are Russian-hacking groups that have a reputation of targeting critical infrastructure and foreign government organizations. Both also have potential ties to the Russian government, although the Russian government has had a

[116] This is noted in the *Definitions* section of the literature review.

record of denial. Further, the malware NotPetya was used in 2017 to affect a variety of critical infrastructure and large corporations including airports and government agencies around the world. This led to about $10 billion dollars in recovery cost. But, no direct use of force was used nor did it directly lead to any deaths. Although it is key to consider how thousands of individuals losing power may affect their lifestyle and may even indirectly lead to loss of life, according to the current framework such action would not be considered an 'armed attack.' In the literature review, it was noted that after legal review under the Obama administration, United States officials began to recognize cyber attacks under Article 51 for self defense if such attacks damaged critical infrastructure. In this example, there was critical infrastructure damaged but since that view point was not necessarily adopted internationally it is not applied in that way to this study.

The implications of this trend, as illustrated in both case studies, are that the existing framework of 'armed attack' does not match up with attacks that occur in the cyber domain even if they parallel or in some way play a role in kinetic attacks like seen in the cases studied. This speaks to the part of the hypothesis that looks at the existing framework applying to kinetic attacks versus cyber attacks. Malicious cyber activity, such as the ones described in the case studies, are often categorized as 'attacks' because they negatively impact large groups of people in an effort to achieve some political goal. But if they do not properly fall into a framework that has been used to deal with armed conflict on an international scale, it is difficult to predict a balanced response to such action. This is a reason why other countries may be hesitant to respond; they do not know what the rules are.

A common issue that can be seen is an issue of attribution. As previously noted in the literature review section of the paper, one of the key differences between kinetic and cyber

attacks is the concrete, direct nature of the kinetic domain versus the fluid, often indirect nature of the cyber domain. There is no doubt when Russia sends military troops across the border to Ukraine that the Russian government is behind such action. When a group such as APT28, a group known to have ties with the Russian government, is suspected of committing a cyber attack in the midst of a conflict between Georgia and Russia one can assume that the Russian government has some role in the attack. But it would seem that the international community would have some hesitation to act solely on grounds of suspected attribution.

How does the International Community respond?

Table 3: International Community Response Ranking

	Kinetic	**Cyber**
Georgia	Intervention	None-Verbal Condemnation
Ukraine	Intervention	Verbal Condemnation

To analyze the international response to the kinetic and cyber attack in Georgia and Ukraine, a ranking system is used. The scale is as follows: *none*, *verbal condemnation*, *intervention*[117]. The results are summarized in Table 3 above. Based on the Georgia case study, EU coordinated a ceasefire between the two countries. The United States also sent aid to Georgia. A delegation of diplomats was sent to Georgia by the EU and the US to mitigate military tensions. Although no direct military action had to be taken by international forces, financial and diplomatic actions were effective in concluding the fighting. Direct intervention from the international community was necessary in stopping the military conflict between Georgia and Russia.

[117] Intervention can include economic sanctions, financial or other support, or physical involvement.

The cyber attacks in Georgia occurred just prior to the escalation of military conflict. Government, media, and transportation company networks were hacked. Computer security experts confirmed that malicious computer programs were staged leading up to the kinetic attacks. The international community stayed mostly silent on the issue at the time. In the aftermath, there was some verbal acknowledgement and Table 3 attempts to reflect that by noting a cross over between no response and verbal condemnation. Could the situation play out differently if the malicious cyber activity was properly acknowledged by the international community? It is possible but considering the variety of other factors that could have been involved it is impossible to provide a concrete answer within this research study.

Looking at the Ukraine case study, there was direct intervention when it came to the kinetic attacks. NATO ordered Russia to withdraw its troops from Ukraine and the United States offered financial support to Ukraine. President Obama also declared a national emergency in regard to the circumstances in Ukraine. With the conflict intensifying, the United States imposed economic sanctions on Russia. Cyber attacks were acknowledged with verbal condemnation. Most U.S. officials were hesitant, at first, to make any official comments on the attacks as they felt like there was a lack of evidence for attribution. Only when the attacks intensified to the point of financially impacting the international community did the United States turn to verbally condemning the actions taken by Russia, although once again Russia denied its involvement. This raises an interesting point. When the cyber attacks affected Ukraine directly and Ukrainian investigators blamed Russia, the international community was hesitant to back them in condemning Russia. But when the attacks grew to a more international focus with billions of dollars in damages and recovery, the world grew more interested. Countries promised international consequences. Was it more clear on an international scale that countries can

respond? In addition to attribution once again being an area of concern, it would seem like level of international impact or damage also seemed to play a role. This would be another reason to question the applicability of the existing framework. Countries could be hesitant to act because they are not sure when the legal guidelines apply. This was an issue area that the experts behind the Tallin Manual attempted to tackle. They wrestled with trying to apply the existing framework to cyber activities, but was that sufficient when response action is still not clear?

Congressional Hearings

The United States Senate held congressional hearings to discuss both the Georgia conflict and the ongoing Ukraine conflict. The main focus of the hearings was to discuss developments on the issue at hand, consequences, and potential avenues of response by the United States and its international partners. A close reading was conducted of the chosen primary sources and several key themes were drawn out as highlighted in the data section above. The key themes highlighted a potential trend of how the United States approaches conflicts that involve both kinetic and cyber components.

There are several key observations that can be drawn from the content analysis conducted on the congressional hearings. First, there is a clear focus on military and political conflict over cyber conflict. In the testimonies on the situation in Georgia, the topic of military conflict is discussed 96 times. Meanwhile, the cyber conflict topic is discussed 17 times. For the Ukraine situation, there is a smaller but still rather significant margin between the two.[118] The second Ukraine hearing entitled "Russian Influence and Unconventional Warfare Operations in The 'Gray Zone': Lessons From Ukraine," provides the smallest margin between the military and cyber conflict code count. At close read, there are some key observations that could be drawn

[118] If one had to predict why the margin was smaller for the Ukraine situation was because there was a larger amount of cyber attacks that occurred and the situation lasts significantly longer than the Georgia situation.

here because this hearing touches on the topic of how unconventional warfare, such as cyber activity and disinformation campaigns, were used to Russia's advantage before the international community could respond by traditional means. Interestingly, this hearing takes places the latest (in 2017) in comparison to the other hearings which take place between 2008 and 2014. It is worthwhile to consider if timing plays a role here. In 2017, it is quite possible that officials are becoming more aware of the looming possibilities of cyber conflict and seeing it play out in actions in such instances as the Ukraine conflict. Some of the testimony during the hearing touches on motivations for Russia to conduct cyber attacks or exploitations. The motivation can be predicted to be similar to that of kinetic attacks in the sense that a certain country aims to achieve particular political goals. If the end goal is the same for these difference forms of attack, it is critical to consider how this may impact response.

What the code count fails to show on the surface, but what can be identified at close read of the testimonies, is that the response is mostly focused on financial assistance and diplomatic intervention when it comes to military or political conflict. The topic of cyber conflict, when acknowledged, revolves around how the United States and the international community should respond. It is interesting to note, that in comparison to the case studies where there is very little direct response to the cyber attacks, the testimonies do acknowledge the cyber threat and discuss response. One of the key issue areas that is identified is that the United States and the international community need to prepare to respond to such attacks in the future. This could lead one to believe that officials understand the cyber threat, they are just still tackling with how to properly deal with it.

What has been learned?

As a reminder the hypothesis for this research project was due to the lack of concrete nature to the cyber domain and lack of applicability of the current conventional warfare framework, the response to cyber attacks is not as direct and persistent as with conventional attacks. It is clear that cyber attacks are addressed in a different manner than conventional attacks and it is possible that, in part, this occurs due to lack of applicability of the current conventional warfare. But a few observations have been drawn out of the data analysis that were not the focus of the hypothesis but seem to play a key role in the issue area.

First, the issue of attribution seems to play a central role in the response delay faced by cyber attacks. This likely stems from the fluid nature of cyber attacks, as opposed to the more concrete nature of kinetic attacks. International actors are hesitant to respond when attacks are not clearly attributed to a certain entity.

Second, level of international impact plays a role. This seems to stem from the idea of a lack of framework for cyber attacks. International actors do not know how to respond because they do not know the rules they should be following when it comes to cyber attacks. When does everybody agree that a line has been drawn? Is it when a community is left without power for 24 hours or when there is loss of life? Cyber attacks operate in their own domain and therefore it seems like they need their own rulebook. This is highlighted by the fact that cyber attacks do not fall under the current definition of 'armed attack.' If they do not, countries are hesitant to act in self-defense but defense is clearly needed to send a message to malicious state actors.

Finally, the congressional hearings were able to highlight that officials acknowledge that both a cyber and kinetic conflict exist. But they group them separately and talk about response separately. This is revealed from close reading of the hearings, but excludes the hearing entitled "Russian Influence and Unconventional Warfare Operations in the 'Gray Zone': Lessons From

Ukraine" because, as mentioned previously, this hearing engaged more with the concept of cyber conflict. This again highlights that the cyber domain is unique and needs its own framework to function. The United States, as displayed in the hearings, acknowledges that there is work to be done in the cyber domain.

Based on lack of applicability to the categorization of an 'armed attack,' clear difference in international response, and acknowledgement by United States officials that there is work in the cyber domain that needs to be done, it can be seen that a new framework is required to deal with cyber conflict on the international stage. Some researchers have argued for amending the current framework, some have argued that malicious cyber activity should not even be considered a domain of war. Based on the data presented in this study, it can be argued that amending the current framework is not enough. A new framework needs to be established where attribution, what level of cyber attack justifies international response, and how the international community should prepare for future cyber attacks are all addressed.

Conclusion

Limitations

As evident through the research process described above, the cyber field is constantly changing. It is not concrete in nature and new cyber interactions between states reveal new potential capabilities. It is currently not clear what each state is capable of when it comes to cyber actions. Therefore, this study was limited by the lack of accessibility to the potentially most recent information on the topics, as well as in case study selection. There are not many incidents of kinetic and cyber attacks occurring under the same conflict. This limited selection makes it difficult to understand if the conclusions drawn above in the discussion section are applicable to the cyber domain in general. It also important to consider that this understanding is

likely to grow and change as new information about the cyber domain is obtained and understood by researchers.

Due to constraints placed on this research project, a limited number of congressional hearings could be selected for content analysis. Although, the patterns that were noted spanned the majority of the testimonies, it would be interesting to expand on this analysis to understand if this pattern would continue with analysis of more primary sources.

Future Research

As acknowledged in the limitations subsection above, the cyber domain is constantly evolving. This research serves to be a foundation for a growing research topic that will evolve as the cyber domain itself evolves and as asymmetric warfare becomes a continued focus of malicious state and non-state actors. This research paper acknowledged the need for a cyber attack framework for international response. Such a framework would ideally promote accountability on the part of nation states that currently remain non-compliant in their cyber domain actions. Further research can look to what a framework like this should entail and what needs to be done for it be developed. A framework to address this issue can take on several forms whether it is legal guidance set forth by international organizations in coordination with nation states or some form of a specific, agreed upon treaty or document between nation states. Further research would entail understanding what would work best in this regard. Understanding case study situations like the ones used for this study can help the United States and its international allies understand what kind of unique issues cyber attacks raise in their relationship with kinetic attacks and conflict with other nation states. As cyber attacks between nation states are on the rise, this issue becomes more urgent. The international community needs to be

prepared to respond to malicious cyber activity in order to set the norm for how to behave in cyberspace.

Bibliography

Applegate, Scott. “The Dawn of Kinetic Cyber.” Center for Secure Information Systems, 2013.

BBC. “Ukrainian Crisis Timeline.” BBC News, 2014. https://www.bbc.com/news/world-middle-east-26248275.

BBC. “Ukraine power cut ‘was cyber-attack’.” BBC News, 2017. https://www.bbc.com/news/technology-38573074.

BBC. “UK and US blame Russia for ‘malicious’ NotPetya cyber-attack.” BBC News, 2018. https://www.bbc.com/news/uk-politics-43062113

CBS. “Russian Bombs Georgia Targets.” CBS, 2008. https://youtu.be/JN8iRDYf5ew.

Cerulus, Laurens. “How Ukraine became a test bed for cyberweaponry.” Politico, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

CNN Editorial Research. “2008 Georgia Russia Conflict Fast Facts.” CNN World, 2021. https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html

Council on Foreign Relations. “Ukraine in Crisis.” Council on Foreign Relations, 2014. https://www.cfr.org/backgrounder/ukraine-crisis.

Dipert, Randall. “The Ethics of Cyberwarfare.” Journal of Military Ethics, 9 no. 4 (December 2010). DOI:10.1080/15027570.2010.536404

European Union Council. “Independent International Fact-Finding Mission on the Conflict in Georgia.” European Union. 2009.

Finlay, Christopher. “Just War, Cyber War, and the Concept of Violence,” 357-376. Springer, 2018.

Handler, Stephenie. “The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare.” Stanford Journal of International Law 208, no. 48 (January 2012): 209-237.

Hayward, Ryan. “Evaluating The ‘Imminence’ Of A Cyber Attack For Purposes Of Anticipatory Self-Defense.” Columbia Law Review 117, no. 2: 1-18.

Hughes, Rex. “Towards a Global Regime for Cyber Warfare,” 106-116. IOS Press, 2009.

International Committee of the Red Cross. “Geneva Convention Relative to the Protection of Civilian Persons in Time of War.” International Committee of the Red Cross, 1949.

International Committee of the Red Cross. “Protocol Additional to the Geneva Conventions of

12 August 1949, and relating to the Protection of Victims of International Armed Conflicts." International Committee of the Red Cross, 1977.

Junio, Timothy J.. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." Journal of Strategic Studies 36 (2013): 125 - 133.

Kang, Jaewon. "Here's what you need to know about Ukraine crisis." CNBC News, 2014. https://www.cnbc.com/2014/04/15/key-events-you-need-to-know-about-ukraine-crisis.html

Libicki, Martin. "Correlations Between Cyberspace Attacks and Kinetic Attacks," 199-211. Center for Cyber Security Studies, 2020.

Liff, Adam. "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio." Journal of Strategic Studies, 36, no. 1. (February 2013): 134-139. DOI: 10.1080/01402390.2012.733312.

Markoff, John. "Before the Gunfire, Cyberattacks." The New York Times, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html

Masters, Jonathan. "Ukraine: Conflict at the Crossroads of Europe and Russia." Council on Foreign Relations, 2020. https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia.

Menn, Joseph. "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government." LA Times, 2008. https://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

National Initiative for Cybersecurity Careers and Studies. "Cybersecurity Glossary." Cybersecurity and Infrastructure Security Agency, 2021.

National Research Council. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," 29-52. The National Academies Press, 2014.

Nye, Joseph. "Only a credible threat of response can deter cyber." News Bank, 2008.

Obama, Barack. *Executive Order Declaring a National Emergency With Respect To The Situation In Ukraine*. Washington DC: Government Printing Office, 2014.

Park, Donghui & Michael Walstrom. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." JSIS, 2017. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Patterson, Ryan. "Silencing the Call to Arms: A Shift Away From Cyber Attacks As Warfare." Loyola of Los Angeles Law Review 48(969) (2015): 969-983.

Phillips, Andrew. "The Asymmetric Nature of Cyber Warfare." U.S. Naval Institute 138, no.10 (2012): 10.

Reuters Staff. "Factbox: Facts about the 2008 War in Georgia." Reuters. (2009). https://www.reuters.com/article/us-georgia-war-conflict-sb/factbox-facts-about-the-2008-war-in-georgia-idUSTRE5732TH20090804.

Rid, Thomas. *Cyber war will not take place: What is Cyber War?* (Oxford University Press, 2013), 1-10.

Schmitt, Michael. "Attack as a Term of Art in International Law: The Cyber Operations Context," 283- 293. Proceedings of the 4th International Conference on Cyber. United States Naval War College International Law Department, 2012.

Sloan, Elinor C. "Modern Military Strategy: Cyberwar," 142-159. Routledge, 2017.

The NATO Cooperative Cyber Defence Centre of Excellence. "NotPetya and WannaCry Call for a Joint Response from International Community." CCDCOE, 2017. https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/

United Nations. "Charter of the United Nations." Article 2. United Nations, 1945.

United Nations. "Charter of the United Nations." Article 51. United Nations, 1945.

U.S. Congress. Senate. Committee On Armed Services. *The Current Situation in Georgia And Implications For U.S. Policy*. 110th Cong., 2nd sess., September 9, 2008.

U.S. Congress. Senate. Committee On Foreign Relations. *Developments in Ukraine*. 113th Cong., 2nd sess., June 5, 2014.

U.S. Congress. Senate. Committee On Foreign Relations. *Russia's Aggression Against Georgia: Consequences And Responses*. 110th Cong., 2nd sess., September 17, 2008.

U.S. Congress. Senate. Committee On Armed Services: Subcommittee on Emerging Threats and Capabilities. *Russian Influence and Unconventional Warfare Operations in The 'Gray Zone': Lessons From Ukraine.* 115th Cong., 1st sess., March 29, 2017.

Volz, Dustin & Sarah Young. "White House blames Russia for 'reckless' NotPetya cyber-attack." Reuters, 2018. https://www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.

Walker, Shaun. "Ukraine crisis: emergency NATO, UN, and EU meetings after Russian invasion

claim." The Guardian, 2014. https://www.theguardian.com/world/2014/aug/28/ukraine-russia-emergency-un-nato-eu-meetings-invasion-claim

Waxman, Matthew. "Cyber Attacks as 'Force' Under UN Charter Article 2(4). Columbia Law School, 87(43) (2011): 43-54.

Welch, Larry. "Cyberspace- The Fifth Operational Domain," 2-7. The Institute for Defense Analysis, 2011.

Zinets, Natalia. "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'." Reuters, 2016. https://www.reuters.com/article/uk-ukraine-crisis-cyber-idUKKBN14I1Q9

CV

Nicole Finkel is from Finksburg, Maryland. She is a graduate student at Johns Hopkins University studying Global Security with expected graduation of Summer 2021. Nicole has an undergraduate degree from George Washington University where she studied political science with a minor in creative writing.